REMARKS

Claim Rejections - 35 USC §103

The examiner rejected claims 1, 10-15, 17, 26-31 under 35 USC §103(a) as unpatentable over Brown et al (5,892,826) in view of Lewis (5,734,819). The applicant respectfully disagrees.

Regarding claim 1, the examiner asserts that Brown discloses encryption circuitry but concedes that Brown does not teach to authenticate a device that provides plaintext data before enabling the encryption circuitry. The examiner asserts that Brown could be modified in view of Lewis to arrive at the claimed invention since Lewis discloses to authenticate a device using a unique chip identifier. The examiner relies on a motivation for this modification in that it "would further improve the security of the system from cryptanalysis attacks."

The rejection should be withdrawn because the examiner has failed to make a prima facie case of obviousness since the prior art references when combined do not teach all of the claim limitations, nor is there a motivation taught by the relied upon prior art to make the modification suggested by the examiner (MPEP 2143).

Combining Brown with Lewis will not teach all of the claim limitations. The examiner concedes that Brown does not teach to authenticate a device providing plaintext data before enabling an encryption circuit. Further, Lewis does not disclose or suggest to authenticate a device providing plaintext data to an encryption circuit; rather Lewis discloses to authenticate a system before allowing software to run on the system. The mere fact that Lewis discloses to authenticate a system before allowing the system to execute software is not the same or even similar to authenticating a device that provides plaintext data before allowing an encryption circuit to operate.

On page 1, lines 28+, of applicant's specification the drawbacks of Lewis are discussed:

> "U.S. patent number 5,743,819 (the '819 patent) discloses a software program executing on a CPU which provides system operation validation in order to prevent the software program from executing on unlicensed computer systems. The validation method requires reading a unique chip identifier (chip ID) stored in a system device, and a corresponding chip ID and an encrypted code stored in a non-volatile memory. The encrypted code, termed a message authentication code or MAC, is generated based on the chip ID using a secret key. The '819 patent relies on uncompromised secrecy of the secret key to prevent tampering which could circumvent the validation process.
>
> The '819 patent is susceptible to a probing attacker attempting to discover the secret key by performing a chosen plain-text attack. For example, a probing attacker could tamper with the cryptosystem to generate chosen plaintext by modifying the chip ID stored in the non-volatile memory and then evaluate the resulting MAC generated by the encryption process. Further, a probing attacker could monitor the software program as it executes on the CPU in order to observe how the chosen plaintext is being encrypted using the secret key. If the secret key is discovered, the security of the system is compromised since the chip ID and corresponding MAC could be altered without detection."

The invention recited in claim 1 overcomes the drawbacks of Lewis by protecting against chosen plaintext attacks by authenticating <u>the device which provides plaintext data to an encryption circuit before enabling operation of the encryption circuit</u> (see page 3, lines 27+, of applicant's specification). Nothing in Lewis would suggest this modification to the prior art.

The examiner has failed to establish a prima facie case of obviousness since Lewis does not disclose or suggest to authenticate a device providing plaintext to an encryption circuit. The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification. (<u>In re Fritch</u> 972 F.2d 1260; 23 U.S.P.Q.2D (BNA) 1780 (1992).) Further, the motivation to improve security as suggested by the examiner comes only from applicant's own disclosure which cannot be used as prior art against the claims. The rejection should be withdrawn since the examiner is employing improper hindsight.

The examiner rejected claims 2 and 9 under 35 USC §103(a) as unpatentable over Brown in view of Lewis and further in view of Le Rue (5,694,469). The applicant respectfully disagrees. Le Rue does not disclose or suggest to authenticate a device providing plaintext data to an encryption circuit, or to authenticate the device receiving the encrypted data. The rejection should be withdrawn.

The rejection of the remaining claims should be withdrawn for the reasons set forth above.

CONCLUSION

The above amendments to the specification do not add new matter or raise new issues; the applicant respectfully requests the amendments be entered. In view of the foregoing remarks, the rejections should be withdrawn. In particular, the relied upon prior art does not disclose or suggest to authenticate a device which provides plaintext data to an encryption circuit. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 4/22/04 By:

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

4/22/04 Howard H. Sheerin
(Date) (Print Name)

(Signature)